

1 BRIAN J. STRETCH (CABN 163973)  
United States Attorney

2 BARBARA J. VALLIERE (DCBN 439353)  
3 Chief, Criminal Division

4 JULIE D. GARCIA (CABN 288624)  
Assistant United States Attorney

5 450 Golden Gate Avenue, Box 36055  
6 San Francisco, California 94102-3495  
Telephone: (415) 436-6758  
7 FAX: (415) 436-7234  
Julie.Garcia@usdoj.gov

8 Attorneys for United States of America

9 UNITED STATES DISTRICT COURT  
10 NORTHERN DISTRICT OF CALIFORNIA  
11 SAN FRANCISCO DIVISION

12 IN THE MATTER OF THE SEARCH OF )  
13 A RESIDENCE IN APTOS, )  
14 CALIFORNIA 95003 )  
15 )  
16 )  
17 )  
18 )

CASE NO. 17-mj-70656 JSC

UNITED STATES' REPLY IN SUPPORT OF  
APPLICATION FOR AN ORDER UNDER THE  
ALL WRITS ACT REQUIRING DEFENDANT  
SPENCER TO ASSIST IN THE EXECUTION  
OF A SEARCH WARRANT

**FILED**

DEC 22 2017

SUSAN Y. SOONG  
CLERK, U.S. DISTRICT COURT  
NORTHERN DISTRICT OF CALIFORNIA



**TABLE OF CONTENTS**

I.	INTRODUCTION .....	1
II.	ARGUMENT .....	1
A.	The government has shown that the requested relief is necessary and appropriate. ....	1
B.	The requested relief would not violate Spencer’s Fifth Amendment privilege against self-incrimination.....	4
1.	<i>Fisher</i> and its progeny set forth the proper framework for applying the Fifth Amendment privilege to the compelled production of evidence. ....	4
2.	Applying <i>Fisher</i> , the potentially testimonial aspects of the act of production are possession and control of the devices, knowledge of the passwords, and that they contain child pornography. ....	6
3.	The government has shown with “reasonable particularity” that each of the potentially testimonial components of the act of production is a foregone conclusion. ....	7
III.	CONCLUSION.....	9

**TABLE OF AUTHORITIES**

**FEDERAL CASES**

*Doe v. United States*, 487 U.S. 201 (1988)..... 4, 5

*Fisher v. United States*, 425 U.S. 391 (1976)..... 4, 7

*Gilbert v. California*, 388 U.S. 263 (1967)..... 6

*Riley v. California*, 134 S. Ct. 2473 (2013) ..... 5

*United States v. Apple MacPro Computer et al.*, 851 F.3d 238 (3d Cir. 2017)..... 4, 9

*United States v. Cotterman*, 709 F.3d 952 (9th Cir. 2013) ..... 5

*United States v. Dionisio*, 410 U.S. 1 (1973)..... 6

*United States v. Doss*, 563 F.2d 265 (6th Cir. 1977) ..... 5

*United States v. Greenfield*, 831 F.3d 106 (2d Cir. 2016) ..... 9

*United States v. New York Tel. Co.*, 434 U.S. 159 (1977) ..... 4

*United States v. Sideman & Bancroft, LLP*, 704 F.3d 1197 (9th Cir. 2013) ..... 7, 9

*United States v. Wade*, 388 U.S. 218 (1967) ..... 6

**FEDERAL STATUTES**

28 U.S.C. § 1651 ..... 1

1 The United States of America hereby submits this reply in support of its application under the  
 2 All Writs Act, 28 U.S.C. § 1651, for an order requiring defendant Ryan Michael Spencer to assist in the  
 3 execution of a federal search warrant by producing in a fully unlocked and unencrypted state three  
 4 electronic devices seized and authorized for search under a warrant issued by this Court in Case No. 17-  
 5 mj-70656 JSC.

## 6 **I. INTRODUCTION**

7 The defense insists that the government has not shown that the requested relief is “necessary” or  
 8 “appropriate” as required by the All Writs Act because it has not shown that it has exhausted all other  
 9 methods of accessing the Subject Devices, such as seeking “backdoor” access through the developers of  
 10 the encryption software. In fact, all of the FBI’s standard forensic methods for accessing the devices  
 11 have failed, and there is no “backdoor” to encryption software like VeraCrypt. If the Court does not  
 12 grant the requested relief, the search warrant will be frustrated.

13 The defense further asserts that the government has not shown that all of the facts implicitly  
 14 communicated by the act of producing the Subject Devices in an unencrypted state are foregone  
 15 conclusions and that, regardless, the foregone conclusion doctrine cannot “supersede” Spencer’s Fifth  
 16 Amendment protections. But the defense misunderstands the foregone conclusion doctrine, which is not  
 17 an exception to the Fifth Amendment but an application of it. Where the government can show with  
 18 “reasonable particularity” that any potentially testimonial aspects of the act of production are foregone  
 19 conclusions, the act of production is not sufficiently “testimonial” to merit Fifth Amendment protection.  
 20 Here, the government has more than met its burden of showing with reasonable particularity that  
 21 Spencer possessed and controlled the devices, that he can access them, and that they contain child  
 22 pornography. Accordingly, the Court should order the requested relief.

## 23 **II. ARGUMENT**

### 24 **A. The government has shown that the requested relief is necessary and appropriate.**

25 The defense asserts that the government has not shown that it is entitled to relief under the All  
 26 Writs Act because it has not shown that the requested relief is “necessary or appropriate.” Opp. at 5. In  
 27 particular, the defense asserts that the government has shown only “minimal attempts at decryption” and  
 28

1 therefore has not shown a “pressing” need for Spencer to produce the Subject Devices in an unencrypted  
2 and unlocked state. Opp. at 5-7. In fact, the government has met its burden.

3 First, as set out in the government’s Application, the FBI’s forensic examiners have attempted to  
4 access the encrypted and password-protected portions of the Subject Devices using a variety of forensic  
5 techniques, all of which have failed. See App. at 4. The government did not go into detail regarding the  
6 nature of these forensic techniques because they are law enforcement-sensitive; disclosing the details of  
7 such techniques publicly would make it easier for criminals to develop techniques for avoiding  
8 decryption in the future. For the avoidance of doubt, however, the government submits with this Reply  
9 a Declaration from Special Agent Chris Marceau, the FBI Digital Extraction Technician (“DExT”) who  
10 led the effort to access the Subject Devices. See Ex. A (Marceau Decl.). As Special Agent Marceau  
11 explains, he employed—and exhausted—the authorized DExT practices and procedures in attempting to  
12 access each of the three Subject Devices. See *id.* at ¶¶ 6-11. None of these attempts was successful.  
13 *Id.* Although the FBI continues to try to access the Subject Devices using additional procedures (the  
14 details of which are also law enforcement-sensitive), the chances of success are slim. See *id.* at ¶¶ 15-  
15 18.

16 Second, the defense incorrectly asserts that the government has “located the encryption  
17 password” for the Transcend 1 TB external hard drive, and that the requested relief therefore is not  
18 necessary or appropriate as to that device. Opp. at 6. In fact, as set out in the Application, the  
19 government located the password for “the Transcend 1 TB external hard drive found in *Petersen’s*  
20 residence”—i.e., the drive that Petersen bought on Amazon and shipped to Spencer, and that Spencer  
21 then filled with child pornography and encrypted. App. at 3 (emphasis added); Marceau Decl. ¶ 8. That  
22 password does not work on *Spencer’s* matching Transcend 1 TB external hard drive, which remains  
23 inaccessible.

24 Third, the defense’s assertion that the government should have contacted VeraCrypt or other  
25 third parties for assistance in accessing the encrypted devices, see Opp. at 7, reflects a fundamental  
26 misunderstanding of the encryption technology at issue here. There is no “backdoor” to VeraCrypt—  
27 and therefore no way for VeraCrypt to assist the government in accessing the encrypted files. Marceau  
28

Decl. ¶ 13. As VeraCrypt explains on its website:

We have not implemented any “backdoor” in VeraCrypt (and will never implement any even if asked to do so by a government agency), because it would defeat the purpose of the software. VeraCrypt does not allow decryption of data without knowing the correct password or key. *We cannot recover your data because we do not know and cannot determine the password you chose or the key you generated using VeraCrypt.* The only way to recover your files is to try to “crack” the password or the key, but *it could take thousands or millions of years* (depending on the length and quality of the password or keyfiles, on the software/hardware performance, algorithms, and other factors).

“Frequently Asked Questions,” *VeraCrypt* (emphases added), available at

<https://www.veracrypt.fr/en/FAQ.html> (last accessed December 14, 2017). Because there is no

“backdoor” to data encrypted with VeraCrypt software, there was and is no reason to seek VeraCrypt’s assistance in decrypting the Subject Devices. With or without VeraCrypt’s assistance, it could take “thousands or millions of years” to crack the password to the encrypted devices. *Id.*; see also Marceau Decl. ¶¶ 15-18 (calculating that, even assuming that the FBI could “guess” 1,000,000 passwords per second, it would take more than 1,649,859 years to enter every conceivable combination of an eleven-character password).

Although it is possible that the “Secret Folder & Photo Video Vault Pro” application has a security flaw that its developer could share with law enforcement, the FBI has thus far been unable to definitively determine who created the application. *Id.* ¶ 15. The application was not sold by an established developer like Google or Apple and is not available for download on any known “app store.” *Id.* Because the FBI has been unable to find a point of contact for the developer, obtaining “backdoor” access to the “Secret Folder & Photo Video Vault Pro” application—a speculative option to begin with—is not a viable way forward.

As the foregoing facts demonstrate, it is exceedingly unlikely that the FBI will be able to access and search the devices unless the Court orders Spencer to produce them in an unencrypted and unlocked state. Moreover, Spencer is not far removed from the underlying controversy, and the requested relief will not impose an unreasonable burden on him; he need only enter the necessary passwords, without being observed by the government, at a time selected by the Court. Accordingly, the government has met its burden of showing that the requested relief is “necessary or proper.” See *United States v. New*

1 *York Tel. Co.*, 434 U.S. 159, 174-75 (1977) (holding that an order requiring a telephone company to  
 2 assist in the installation of a pen register was “clearly authorized by the All Writs Act,” because the  
 3 order was not unreasonably burdensome, the phone company was not so far removed from the  
 4 underlying controversy as to make enforcement unfair, and without such assistance there was “no  
 5 conceivable way” in which the search warrant could be effectuated); *United States v. Apple MacPro*  
 6 *Computer et al.*, 851 F.3d 238, 245 (3d Cir. 2017) (upholding an order under the All Writs Act requiring  
 7 the defendant to produce electronic devices in an unencrypted state; the defendant was not far removed  
 8 from the underlying controversy, compliance with the order required minimal effort, and without the  
 9 defendant’s assistance there was no conceivable way in which the search warrant could be effectuated).

10 **B. The requested relief would not violate Spencer’s Fifth Amendment privilege against**  
 11 **self-incrimination.**

12 **1. *Fisher* and its progeny set forth the proper framework for applying the Fifth**  
 13 **Amendment privilege to the compelled production of evidence.**

14 The defense acknowledges that the Fifth Amendment privilege against self-incrimination applies  
 15 only to an act or communication that is “(1) testimonial, (2) incriminating, and (3) compelled.” Opp. at  
 16 7. The defense also concedes that, under the “foregone conclusion” doctrine set out in *Fisher v. United*  
 17 *States*, 425 U.S. 391 (1976), the government can compel an individual to produce potentially  
 18 incriminating evidence so long as it can show with “reasonable particularity” its independent knowledge  
 19 of any potentially testimonial communications implicit in the act of production. Opp. at 16.

20 After conceding that this is the relevant framework, however, the defense backtracks, cherry-  
 21 picking out-of-context quotations from various lines of cases and attempting to patch them together to  
 22 suggest that encrypted electronic evidence is afforded unique protections under the law. In some  
 23 instances, the defense outright misrepresents the holding of the cases, such as the citation of *Doe v.*  
 24 *United States*, 487 U.S. 201 (1988) (“*Doe II*”), for the proposition that forced decryption “encroaches on  
 25 ‘the right of each individual to a private enclave where he may lead a private life.’” Opp. at 14 (quoting  
 26 *Doe II*, 487 U.S. at 212). In fact, *Doe II* concluded that a court order compelling the target of a grand  
 27 jury investigation to write a letter authorizing foreign banks to disclose records of his accounts did *not*



1 violate his Fifth Amendment privilege against self-incrimination because the letter was “not testimonial  
2 in nature.” *Id.* at 219. The case had nothing to do with encryption, and it certainly did not hold that  
3 ordering someone to decrypt a device categorically violates the Fifth Amendment.

4 The defense attempts to bolster the argument that encrypted evidence is uniquely testimonial by  
5 quoting cases opining that electronic devices are like “personal diaries” that “contain the most intimate  
6 details of our lives,” *Opp.* at 14 (quoting *United States v. Cotterman*, 709 F.3d 952, 964 (9th Cir. 2013)),  
7 and that they “hold for many Americans ‘the privacies of life,’” *id.* at 14-15 (quoting *Riley v. California*,  
8 134 S. Ct. 2473, 2490 (2013)). But the issue in each of those cases was whether a warrantless search of  
9 a defendant’s electronic devices was unreasonable in violation the *Fourth Amendment*, not whether  
10 accessing the devices violated the defendant’s Fifth Amendment privilege against self-incrimination.  
11 *See Riley*, 134 S. Ct. at 2485 (holding that the government must generally obtain a warrant before  
12 searching a cell phone, even when the search is incident to arrest); *Cotterman*, 709 F.3d at 971 (holding  
13 that a border search of electronic devices was reasonable under the Fourth Amendment because it was  
14 supported by reasonable suspicion). These cases have no application here, where the government seized  
15 the Subject Devices pursuant to a valid search warrant issued upon a showing of probable cause.

16 Relying on *United States v. Doss*, 563 F.2d 265 (6th Cir. 1977), the defense further asserts that  
17 “[f]orcing Mr. Spencer to decrypt his devices is the functional equivalent of calling him to testify at  
18 trial,” in violation of his Fifth Amendment privilege. *Opp.* at 22. Again, the defense’s analysis is  
19 flawed. *Doss* held that the government violated the defendant’s *Sixth Amendment* right to counsel and  
20 his Fifth Amendment *due process* rights by calling him before the grand jury to question him secretly,  
21 without counsel present, and without informing him that he had already been indicted. *Id.* at 278-79.  
22 The case did not involve the compelled production of evidence, or even compelled testimony; in fact,  
23 the defendant repeatedly invoked his Fifth Amendment privilege not to testify. 563 F.2d at 267. The  
24 *Doss* analysis is not helpful here, where none of the Sixth Amendment or due process issues is present,  
25 and where Spencer is not being compelled to *testify*, but rather to produce evidence.

26 To be clear, in articulating the foregone conclusion doctrine, the Supreme Court did not create an  
27 exception to the Fifth Amendment, nor did it establish “a more narrow boundary applicable to acts  
28



alone.” *Doe II*, 487 U.S. at 209. The distinction is simply that “verbal statement[s], either oral or written,” will almost always be testimonial, whereas certain nonverbal acts—such as the act of producing evidence—may not be sufficiently testimonial to warrant Fifth Amendment protection. *Id.* at 209-10, 213-14; *see also Gilbert v. California*, 388 U.S. 263, 266-67 (1967) (defendant can be compelled to provide a handwriting sample); *United States v. Dionisio*, 410 U.S. 1, 7 (1973) (defendant can be compelled to provide a voice exemplar); *United States v. Wade*, 388 U.S. 218, 222-23 (1967) (defendant can be compelled to stand in a lineup). Because the relief the government seeks here would require Spencer to produce evidence, the proper framework for analyzing his Fifth Amendment claim is the foregone conclusion analysis set out in *Fisher*.

**2. Applying *Fisher*, the potentially testimonial aspects of the act of production are possession and control of the devices, knowledge of the passwords, and that they contain child pornography.**

The defense purports to identify two ways in which the act of producing the Subject Devices in an unencrypted and unlocked state would be testimonial. First, the defense asserts that the act of producing the Subject Devices in an unencrypted and unlocked state would “implicitly communicate that [Spencer] possessed or controlled” the devices, and that he “could decrypt, retrieve, and examine” their contents. *Opp.* at 12. Second, the defense asserts that the act would be testimonial because “it would translate otherwise unintelligible data into a form that can be used and understood by investigators.” *Id.* at 13. Although the reasoning underlying this second argument is not clear, the defense appears to be asserting that the encrypted files would convey information upon being decrypted, and that this “testimony” merits Fifth Amendment protection.

The defense’s first point is accurate: The act of producing the Subject Devices would, indeed, implicitly communicate that Spencer possessed or controlled the devices, and that he is able to decrypt and access their contents. Moreover, although producing a device in an unencrypted state does not necessarily imply knowledge of the device’s contents, the government recognizes that where a search warrant has been issued for an individual’s device based on probable cause to believe that it contains child pornography, the individual’s ability to produce the device in an unencrypted state will generally

1 provide strong evidence of the individual's knowledge of its contents. Accordingly, as set out in the  
2 government's Application, *see* App. at 14, the government has been proceeding on the assumption that it  
3 must also show that it is a foregone conclusion that the Subject Devices contain child pornography.

4 But the defense's second argument—that the act of decryption is itself “testimonial” as to the  
5 contents of the files—misses the mark. The relevant question is not whether decrypting the devices  
6 would lead to incriminating evidence, but whether the very act of decrypting the devices would  
7 *implicitly* communicate something to the government that it does not already know. *See Fisher*, 425  
8 U.S. at 410-11 (holding that, “however incriminating the contents” of certain subpoenaed tax papers  
9 might be, there was no Fifth Amendment violation where “*the act of producing them*—the only thing  
10 which the taxpayer is compelled to do—[did] not involve testimonial self-incrimination” (emphasis  
11 added)). The act of decrypting a device does not implicitly communicate the contents of each of the  
12 files the device contains, because a limitless variety of digital media—not just the particular files of  
13 child pornography that are on these devices—can be encrypted and decrypted. Indeed, there is no  
14 relevant distinction between producing evidence stored in “Banker Boxes” and “Daytime Planners,” *see*  
15 *United States v. Sideman & Bancroft, LLP*, 704 F.3d 1197, 1200 (9th Cir. 2013), and producing  
16 evidence stored on an encrypted device; in either case, the Court can require the individual to produce  
17 the evidence—however incriminating its contents may be—if the government shows that the facts  
18 implicitly communicated by the act of production are foregone conclusions.

19 **3. The government has shown with “reasonable particularity” that each of the**  
20 **potentially testimonial components of the act of production is a foregone**  
21 **conclusion.**

22 The defense does not contest that the government has shown with “reasonable particularity” its  
23 independent knowledge of Spencer's ownership, possession, and ability to access the Subject Devices.  
24 *See* Opp. at 15-23 (addressing the foregone conclusion issue without mentioning these implicit facts);  
25 *see also* App. at 17-18 (setting out why these facts are foregone conclusions). Instead, the defense  
26 focuses on the last potentially testimonial aspect of the act of production, and insists that the government  
27 has not met its burden of showing with reasonable particularity that the Subject Devices contain child  
28

1 pornography. *See* Opp. at 15-18. None of the defense's arguments withstands scrutiny, however.

2 First, the defense argues that it is not a foregone conclusion that the "Secret Folder & Photo  
3 Video Vault Pro" application contains child pornography because "Mr. Petersen provided no testimony  
4 as to the contents of that folder" and "did not see any images on Mr. Spencer's phone." Opp. at 16, 18.  
5 In fact, however, Petersen explained that Spencer claimed to take sexually explicit photographs of  
6 children and then move the images from his phone's camera roll to an iPhone application that password  
7 protected them. Petersen Decl. ¶ 8. Petersen further stated that Spencer had installed an application on  
8 his iPhone that made the screen go black, as if it were off, while still allowing him to take photographs.  
9 *Id.* at ¶¶ 4-5. Petersen's statements were corroborated when the FBI later discovered on Spencer's  
10 iPhone both the "Spy Camera" application, which allows the user to take photos surreptitiously, and the  
11 "Secret folder & Photo Video Vault Pro" application, an application that password protects images and  
12 videos. *See* App. at 4; *id.* at 5 n.8; Ex. B (Declaration of FBI Special Agent Elizabeth Hadley) at ¶¶ 21-  
13 22. More generally, the recovered Kik messages definitively show that Spencer used his iPhone to take  
14 sexually explicit photographs of children. Not only do the Kik messages contain hundreds of images  
15 that Spencer took and sent to Petersen, but they also capture Spencer himself describing how he used his  
16 iPhone to create child pornography. *See* App. at 8-9 (describing a Kik message exchange in which  
17 Spencer told Petersen that he could "control and take pictures from [his] iPhone" using his watch, such  
18 that if he "left [the phone] in a room propped up" he could take pictures even if he was not in the room);  
19 Hadley Decl. ¶ 19.

20 The defense also argues that it is not a foregone conclusion that the Alienware laptop contains  
21 child pornography, because Petersen was not able to identify which laptop Spencer had used on the day  
22 they met. Opp. at 18. In light of all of the other evidence about the Alienware laptop, however, an  
23 eyewitness identification by Petersen is not necessary. First, Spencer told Petersen that he kept part of  
24 his collection of child pornography in an encrypted portion of his computer's hard drive, Petersen Decl.  
25 ¶ 9, and a portion of the Alienware laptop's hard drive is encrypted. Marceau Decl. ¶ 7(e). Second, the  
26 recovered Kik messages capture Spencer himself claiming to have child pornography on his computer.  
27 *See* App. at 8 (discussing Kik messages in which Spencer bragged that the material "on [his] computer  
28

[was] hot as fuck”); Hadley Decl. ¶ 18. Finally, because there was no other working laptop in Spencer’s room at the time the search warrant was executed, there is no question as to whether the Alienware laptop is the one that Spencer was using as of April 2017 to store part of his collection of child pornography. *See* App. at 4 n.6; Marceau Decl. ¶ 5. Taken together, this evidence shows with “reasonable particularity” that the Alienware laptop contains child pornography.

Finally, the defense argues that the government has failed to meet its burden because, whereas “the main evidence in *Apple Macpro* came from a neutral third party, the defendant’s sister,” here the government is relying on “the representation of a self-interested co-defendant,” Petersen. In fact, the government is relying not only on Petersen’s detailed testimony, but on Spencer’s own words and actions captured in the Kik chats on his phone. *See generally* App. at 5-9; Hadley Decl. ¶¶ 12-20. Moreover, the government has independently corroborated Petersen’s testimony as to each of the Subject Devices. As noted in the preceding paragraphs, the FBI found the “Secret folder & Photo Video Vault Pro” and “Spy Camera” applications on Spencer’s iPhone, corroborating Petersen’s claim that Spencer stored child pornography in a password protected iPhone application and used an application to take photographs surreptitiously. Similarly, Petersen’s claim that Spencer stored child pornography on an encrypted portion of his computer’s hard drive was corroborated when the FBI found an encrypted portion of the Alienware laptop’s hard drive, and when recovered Kik messages captured Spencer repeatedly telling Petersen that he had child pornography on his computer. *See id.* Additionally, Petersen’s claim that he saw Spencer access child pornography on the Transcend 1 TB external hard drive is corroborated by Spencer’s own words, captured in the Kik chats, which definitively show that he stored child pornography on a Transcend 1 TB external hard drive that he had encrypted. *See* App. at 7; Hadley Decl. ¶ 13.

To be entitled to relief, the government need not show that the Subject Devices contain child pornography beyond a reasonable doubt. Instead, the government’s burden is to make that showing with “reasonable particularity.” *Sideman & Bancroft, LLP*, 704 F.3d at 1202; *accord Apple MacPro Computer*, 851 F.3d at 247; *United States v. Greenfield*, 831 F.3d 106, 116 (2d Cir. 2016). For the reasons given above and in the government’s Application, the government has made that showing here.

//

1 **III. CONCLUSION**

2 For the foregoing reasons, the United States respectfully requests that the Court issue an order  
3 pursuant to the All Writs Act requiring defendant Ryan Michael Spencer to assist in the execution of the  
4 search warrant issued in Case No. 17-mj-70656 JSC by producing the Subject Devices in a fully  
5 unlocked and unencrypted state.

6  
7 DATED: December 22, 2017

Respectfully submitted,

8 BRIAN J. STRETCH  
9 United States Attorney

10   
11 JULIE D. GARCIA  
12 Assistant United States Attorney  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

# EXHIBIT A

BRIAN J. STRETCH (CABN 163973)  
United States Attorney

BARBARA J. VALLIERE (CABN 439353)  
Chief, Criminal Division

JULIE D. GARCIA (CABN 288624)  
Assistant United States Attorney

450 Golden Gate Avenue, 11<sup>th</sup> Floor  
San Francisco, California 94102  
Telephone: (415) 436-6758  
FAX: (415) 436-7234  
Julie.Garcia@usdoj.gov

Attorneys for the United States of America

UNITED STATES DISTRICT COURT  
FOR THE NORTHERN DISTRICT OF CALIFORNIA  
SAN FRANCISCO DIVISION

IN THE MATTER OF THE SEARCH OF  
A RESIDENCE IN APTOS,  
CALIFORNIA 95003

No. 17-70656 JSC

DECLARATION OF FBI SPECIAL AGENT  
CHRISTOPHER MARCEAU IN SUPPORT OF  
APPLICATION FOR AN ORDER UNDER THE  
ALL WRITS ACT REQUIRING DEFENDANT  
SPENCER TO ASSIST IN THE EXECUTION OF A  
SEARCH WARRANT

I, Christopher Marceau, hereby declare:

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI") and have been employed by the FBI as such since 2008. I am currently assigned to the squad that investigates Child Exploitation matters in the San Francisco Division. I am a trained Digital Evidence Extraction Technician (DExT), which authorizes me to search, find, and extract digital evidence in support of FBI investigations. As part of my duties as an FBI agent, I investigate criminal violations relating to child exploitation and child pornography, including violations pertaining to the illegal production,

DECLARATION OF CHRISTOPHER MARCEAU  
CR No. 17-70656 JSC



1 distribution, receipt, and possession of child pornography, in violation of 18 U.S.C. §§ 2251, 2252, and  
2 2252A.

3 2. I am the DExT assigned to the above-captioned investigation, which involves defendant  
4 Ryan Spencer, and to investigation number 17-mj-70591 JCS, involving defendant Bryan Petersen.

5 3. As part of the above-captioned investigation, I participated in the execution of the search  
6 warrant executed at defendant Ryan Spencer's home on April 27, 2017.

7 4. The following three electronic devices (among others) were seized from Spencer's  
8 residence:

9 a) A black and green Transcend 1 TB external hard drive with serial number  
10 C842472715. This external hard drive was on Spencer's desk. It is the same make and model as  
11 the Transcend 1 TB external hard drive found in the residence of Spencer's codefendant, Bryan  
12 Petersen.

13 b) A silver and black Alienware laptop, Model P42F, with serial number 451PM32.  
14 This laptop was also on Spencer's desk. I learned from the case agent in this matter, Special  
15 Agent Elizabeth Hadley, that, in an interview, Spencer stated that the PIN for the computer was  
16 "1997."

17 c) A black iPhone 7, Model A1660, with serial number F72SDRNGHG71. This  
18 phone was in Spencer's hand when the other agents and I arrived.

19 5. A black Lenovo laptop was also seized from Spencer's residence. However, this device  
20 had no hard drive in it.

21 **The Transcend 1 TB external hard drive**

22 6. I attempted to access the Transcend 1 TB external hard drive seized from Spencer's  
23 residence using authorized DExT practices and procedures, none of which was successful. The exact  
24 nature of these practices and procedures is law enforcement-sensitive; however, the steps I took included  
25 the following:

26 a) Using FBI-approved tools, I created a forensic image of the Transcend 1 TB  
27 external hard drive. The drive geometry was captured, and the accuracy of the forensic image

1 was verified using an MD5 hash.

2 b) I then employed FBI-approved tools to process the drive. These tools were  
3 unable to read the data on the drive, which appeared to be encrypted.

4 c) Using FBI-approved tools, I then created a clone of the Transcend 1 TB external  
5 hard drive. This process captured the drive geometry, which indicated that the drive contained  
6 913 GB of data—nearly a terabyte.

7 d) I then created a working copy clone of the Transcend 1 TB external hard drive.  
8 Again, the accuracy of the working copy clone was verified using an MD5 hash. I then  
9 attempted to access the device using a list of potential passwords derived from patterns and  
10 profiles developed during the investigation. After attempting to access the device with the tenth  
11 incorrect password, however, VeraCrypt software overwrote the data.

12 e) I then created a second working copy clone of the Transcend 1 TB external hard  
13 drive. Again, the accuracy of the working copy clone was verified using an MD5 hash. I  
14 attempted to open the drive with VeraCrypt using a second set of ten passwords. The drive could  
15 not be accessed, and on the tenth attempt, VeraCrypt again overwrote the data.

16 f) I then examined the unencrypted portion of the Alienware laptop in an attempt to  
17 locate VeraCrypt encryption keyfiles. However, I could not locate any VeraCrypt keyfiles in the  
18 unencrypted portion of the Alienware laptop.

19 g) I continue to attempt to create and access working copy clones of the Transcend 1  
20 TB external hard drive. Given the size of the drive, the nature of the encryption, and the  
21 verification process required to ensure forensic accuracy of the clones, the process takes multiple  
22 weeks. Each time, after entering just ten incorrect passwords, VeraCrypt overwrites the data,  
23 requiring me to begin the process again.

24 h) I have obtained additional FBI-approved and commercially available tools in an  
25 attempt to decrease the amount of time to clone and verify a working copy, thus far without  
26 success.

27 //

1       **The Alienware laptop**

2           7.       I also attempted to access and review the Alienware laptop's hard drive using authorized  
3 DExT practices and procedures, none of which was successful. The exact nature of these practices and  
4 procedures is law enforcement-sensitive; however, the steps I took included the following:

5               a)       I powered on the Alienware laptop and connected to it an FBI drive containing  
6 FBI-approved tools. Using those FBI-approved tools, I observed that the passcode "1997,"  
7 which I understand Spencer provided to the FBI, did unlock the Alienware laptop. I then placed  
8 the Alienware laptop in "airplane mode" and changed the laptop's settings so that the screen  
9 would not lock again. I did not observe any destructive processes running on the laptop.

10              b)       A review of the applications on the Alienware laptop revealed that VeraCrypt  
11 version 1.0.5.0 was running on it. I attempted to access the VeraCrypt software to obtain  
12 passwords and/or encryption keys but was not able to access such items. The exact nature of the  
13 steps I took in an attempt to access the VeraCrypt software is law enforcement-sensitive.

14              c)       Using FBI-approved tools, I then created a forensic image of the Alienware  
15 laptop. The laptop had two separate hard drives. The first was a 1.0 TB Western Digital hard  
16 drive, serial number WX31AC4PVLTO, and the second was a 128GB Samsung SSD, serial  
17 number S1D2NYAG302944. This process captured the drive geometry of each drive, and the  
18 accuracy of the forensic image was verified using MD5 hashes.

19              d)       Using FBI-approved tools, I examined the drives and observed that they contained  
20 ten (10) separate partitions. A "partition" is a section of a hard drive that is isolated from other  
21 sections. In my training and experience, it is unusual to have such a large number of partitions  
22 on a drive.

23              e)       I attempted to access three of the partitions using tools and techniques that are law  
24 enforcement-sensitive. These attempts failed; however, I determined that the partitions are  
25 consistent with encrypted partitions I have encountered in other investigations. I have been  
26 unable to determine whether VeraCrypt or some other encryption software was used to encrypt  
27 the partitions.

1 f) I then processed the image of the Alienware laptop using FBI-approved tools.  
2 However, the encrypted, partitioned drives remained inaccessible.

3 8. On the accessible portion of the Alienware laptop's hard drive, I discovered a file  
4 containing the encryption password to the Transcend 1 TB external hard drive found in Petersen's  
5 residence. The password was eleven characters long and used numbers and upper- and lower-case  
6 letters.

7 **The iPhone 7**

8 9. I also reviewed Spencer's iPhone 7. On that device, I found Kik messages containing  
9 child pornography, including the same messages found on Petersen's phone.

10 10. Installed on the iPhone 7 is a password-protected application believed to be the  
11 application "Secret Folder & Photo Video Vault Pro." The application's icon simply describes the  
12 application as "Folder." This application takes up nearly 20 gigabytes of the phone's memory—more  
13 than any other application.

14 11. I attempted to access the "Secret Folder & Photo Video Vault Pro" application using  
15 authorized DExT practices and procedures, none of which was successful. The exact nature of these  
16 practices and procedures is law enforcement-sensitive; however, the steps I took included the following:

17 a) A logical extraction of the device was created using FBI-approved tools. These  
18 tools were not able to access the data in the "Secret Folder & Photo Video Vault Pro"  
19 application.

20 b) FBI-approved tools were then used to create a physical extraction of the device.  
21 Using the physical extraction, I examined the file structure of the device in an attempt to locate  
22 the password or the encryption keys for the "Secret Folder & Photo Video Vault Pro"  
23 application. I located four files pertaining to the application including file  
24 "info.e2uapp.photosafe"; however, I have not been able to access any of these files.

25 **Continuing efforts to access the devices**

26 12. The FBI continues to try to access the three electronic devices described herein using  
27 additional procedures. The details of these efforts are law enforcement-sensitive.

**Lack of alternative avenues for circumventing encryption**

13. As a DExT, I am familiar with encryption software generally and with VeraCrypt software in particular. On a daily basis, I am responsible for attempting to access the contents of encrypted electronic devices seized by the FBI. In my training and experience, I know that there is no “backdoor” to VeraCrypt, and therefore no way for VeraCrypt to assist the government in accessing the encrypted files. As VeraCrypt explains on its website:

We have not implemented any “backdoor” in VeraCrypt (and will never implement any even if asked to do so by a government agency), because it would defeat the purpose of the software. VeraCrypt does not allow decryption of data without knowing the correct password or key. *We cannot recover your data because we do not know and cannot determine the password you chose or the key you generated using VeraCrypt.* The only way to recover your files is to try to “crack” the password or the key, but *it could take thousands or millions of years* (depending on the length and quality of the password or keyfiles, on the software/hardware performance, algorithms, and other factors).

“Frequently Asked Questions,” *VeraCrypt* (emphases added), available at <https://www.veracrypt.fr/en/FAQ.html> (last accessed December 14, 2017).

14. The FBI has thus far been unable to definitively determine who created the “Secret Folder & Photo Video Vault Pro” application. This application was not sold by an established developer like Google or Apple and is not available for download on any known “app store.”

**Likelihood of determining the encryption passwords with a “brute force” attack**

15. As noted, my review of the Alienware laptop seized from Spencer’s residence revealed a file containing the password to the Transcend 1 TB external hard drive found in Petersen’s residence. That password contained eleven characters, including upper- and lower-case letters and numbers.

16. Based on investigative reports and my conversations with the case agent on this matter, I understand that, according to Petersen, Spencer encrypted the Transcend 1 TB external hard drive for Petersen, and it was Spencer who created the encryption password described in the preceding paragraph.

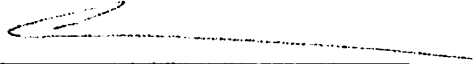
17. In my experience, offenders often use long and complex passwords when attempting to hide child pornography and other contraband. Accordingly, I believe that it is likely that, for his own devices, Spencer used an encryption password of at least the same level of complexity as the password

1 that he provided to Petersen.

2 18. Assuming that Spencer used a password of eleven characters, also with upper- and lower-  
3 case letters and numbers, the total number of potential passwords is  $62^{11}$ , or  
4 52,036,561,000,000,000,000. Even assuming that the FBI could execute a "brute force" attack with an  
5 "guess" rate of 1,000,000 passwords per second, it would take more than 1,649,859 years to enter every  
6 conceivable combination in order to crack the password.

7 I declare under penalty of perjury that the foregoing is true and correct to the best of my  
8 knowledge.

9 Executed on this 22 day of December, 2017, in Campbell, California.

10  
11   
12 Special Agent Christopher Marceau  
13 Federal Bureau of Investigation  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

# **EXHIBIT B**



BRIAN J. STRETCH (CABN 163973)  
United States Attorney

BARBARA J. VALLIERE (CABN 439353)  
Chief, Criminal Division

JULIE D. GARCIA (CABN 288624)  
Assistant United States Attorney

450 Golden Gate Avenue, 11<sup>th</sup> Floor  
San Francisco, California 94102  
Telephone: (415) 436-6758  
FAX: (415) 436-7234  
Julie.Garcia@usdoj.gov

Attorneys for the United States of America

UNITED STATES DISTRICT COURT  
FOR THE NORTHERN DISTRICT OF CALIFORNIA  
SAN FRANCISCO DIVISION

IN THE MATTER OF THE SEARCH OF  
A RESIDENCE IN APTOS,  
CALIFORNIA 95003

No. 17-70656 JSC

DECLARATION OF FBI SPECIAL AGENT  
ELIZABETH HADLEY IN SUPPORT OF  
APPLICATION FOR AN ORDER UNDER THE  
ALL WRITS ACT REQUIRING DEFENDANT  
SPENCER TO ASSIST IN THE EXECUTION OF A  
SEARCH WARRANT

I, Elizabeth Hadley, hereby declare:

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI") and have been employed by the FBI as such since 2009. I am currently assigned to the San Francisco field office in a squad that investigates crimes against children. Since joining the FBI, I have investigated, among other things, federal criminal violations related to child pornography and the sexual exploitation of minors. I have experience investigating violations of child pornography and child exploitation and have reviewed numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in various forms of media,

DECLARATION OF ELIZABETH HADLEY  
No. 17-mj-70656 JSC

1 including computer media. I have participated in the execution of numerous search warrants conducted  
2 by the FBI and in the seizure of computer systems and other types of digital evidence.

3 2. I am the case agent assigned to the above-captioned investigation, which involves  
4 defendant Ryan Spencer, and to investigation number 17-mj-70591 JCS, involving defendant Bryan  
5 Petersen.

6 **Search of Bryan Petersen's residence**

7 3. On April 26, 2017, other FBI agents and I executed a search warrant at the home of  
8 Bryan Petersen in Tiburon, California. *See* Case No. 17-mj-70591 JCS. Petersen was present and  
9 agreed to be interviewed. He admitted to me that he possessed images and videos containing child  
10 pornography and that he had exchanged such materials with individuals he had met on the internet,  
11 including defendant Spencer. Petersen explained to me that, approximately twelve to eighteen months  
12 prior, he had ordered an external hard drive from Amazon.com and had it delivered to Spencer, who—  
13 based on the two men's prior agreement—then filled the hard drive with child pornography. Petersen  
14 further explained that, at some point thereafter, he had traveled to Aptos, California, where he met  
15 Spencer and retrieved the external hard drive. Petersen estimated that the external hard drive contained  
16 between 10,000 and 100,000 images and videos of child pornography.

17 4. Petersen told me that Spencer worked as a babysitter and took photos and videos of some  
18 of the children while they were naked. Petersen stated that he had received many images of naked  
19 prepubescent children from Spencer via an internet messenger application called Kik. Petersen noted  
20 that Spencer was attracted to children as young as four to eight years old and that Spencer claimed to  
21 have molested a child while the child was asleep. Petersen also admitted that he himself had taken  
22 photographs of some of the children he babysat while the children were naked, and that he had sent  
23 those photos to Spencer.

24 5. Several electronic devices were seized from Petersen's residence, including a Transcend  
25 1 TB external hard drive.

26 6. At the end of the interview, Petersen provided the names and contact information of his  
27 victims and the passwords for all of his electronic devices.

1           **Review of Petersen and Spencer's Kik chats**

2           7.       I personally reviewed the Kik messages on Petersen's iPhone. These included Kik  
3 messages that he had exchanged with Spencer from April 1 to 26, 2017. The messages revealed that  
4 Petersen and Spencer actively solicited babysitting jobs—Petersen in Tiburon and Spencer in Santa  
5 Cruz—in order to have physical contact with children, to take sexually explicit photos of them, and to  
6 share those photos with each other. In one Kik exchange, for example, Petersen reported that one of the  
7 children he was babysitting was "laying on [Petersen's] lap fondling himself." Petersen promised that  
8 he would "send pics" the next day. Spencer asked whether Petersen had "anything naked," to which  
9 Petersen responded, "Some." Petersen then sent Spencer a photograph of two prepubescent boys naked  
10 in a bathtub, with penis and buttocks visible, and additional photographs of prepubescent boys changing  
11 into their pajamas. Spencer wrote back that the pictures were "hot," and that he wanted more images  
12 because the children were "smoking."

13           8.       In subsequent exchanges, Spencer sent Petersen several images of prepubescent boys  
14 changing after a swim class, including several in which the boys' penises were visible. Shortly  
15 thereafter, Spencer sent Petersen sixteen images of two prepubescent boys changing their clothes in a  
16 camp cabin, including several in which those boys' penises were also visible. When he sent the images  
17 to Petersen, Spencer remarked that he had seen one child's "stuff" briefly but that it was difficult  
18 because the child was "good at changing [clothes]." In other exchanges, Spencer described his attempts  
19 to get the children he was babysitting to become more comfortable being naked with him and his  
20 attempts to spend time in bed with them. According to Spencer's messages, at least one of these  
21 children was still in diapers.

22           **Search of Ryan Spencer's residence**

23           9.       On April 27, 2017, other FBI agents and I executed a search warrant at the home of  
24 defendant Ryan Spencer in Aptos, California. *See* Case No. 17-mj-70656 JSC. Spencer answered the  
25 door to the detached garage that served as his bedroom and, upon realizing that it was the FBI, attempted  
26 to shut the door again. Other agents and I prevented the door from shutting and detained Spencer while  
27 we searched his room, where we found, as relevant here:

1 a) A silver and black Alienware laptop, Model P42F, with serial number 451PM32.

2 This laptop was on Spencer's desk. In an interview that morning, Spencer admitted ownership  
3 of the laptop and told us that the PIN to it was "1997."

4 b) A black and green Transcend 1 TB external hard drive with serial number

5 C842472715. This external hard drive was on the same desk as the Alienware laptop.

6 c) A black iPhone 7, Model A1660, with serial number F72SDRNGHG71. This

7 iPhone 7 was in Spencer's hand when we entered his room. Spencer admitted that the phone was  
8 his and later, through counsel, provided the passcode to bypass the lock screen.

9 **Older Kik messages recovered from Petersen's and Spencer's devices**

10 10. As part of this investigation, I used Cellebrite, a mobile device analysis tool, to access the  
11 Apple iPhone 7, Model A1660, with serial number F72SDRNGHG71, that was seized from the  
12 residence of Ryan Spencer.

13 11. The Cellebrite extraction report recovered deleted Kik messages between Petersen and  
14 Spencer, some dating back to early 2016. I personally reviewed all of the recovered messages.

15 12. In January 2016, Spencer bragged about the size of his child pornography collection,  
16 saying that it was "like 300 gigs [gigabytes]" and noting that he needed a new external hard drive."

17 13. In an exchange from the next month, Spencer sent more than a dozen images of child  
18 pornography to Petersen, asserting that the images were "a fraction" of what he had. When Petersen  
19 asked where Spencer recommended keeping the child pornography, Spencer responded, "Haha an  
20 external drive. Encrypted up the ass. That you can smash with a hammer at a moment's notice."  
21 Petersen wrote back that he did not know how to set up that kind of encryption, and Spencer responded:  
22 "I could very easily set it up for u." Spencer opined that he had "some flaws in [his] system" for storing  
23 child pornography but that he was "working on it." Spencer added that, in addition to his hard drive, his  
24 computer "might be incriminating too."

25 14. A few days later, Spencer told Petersen that he had recently had sex with a fifteen-year-  
26 old boy. Spencer responded: "I have so many pics I have to download on my computer lol." When  
27 Petersen asked whether the photos were ones that Spencer had taken or ones he had "found," Spencer  
28

1 responded: "Both."

2 15. In March 2016, Spencer wrote to Petersen that he had gotten a new, 1 TB hard drive,  
3 which was twice the size of his old one, and that he was "[e]ncrypting it and making it [his] bitch!!"  
4 Spencer offered to let Petersen borrow his old hard drive and again offered to help Petersen create "a  
5 computer vault" for storing his collection. Petersen responded that he did not yet have a collection on a  
6 hard drive and that he was not sure he preferred such images to those of 18-year-olds who looked young.  
7 Spencer responded: "I can make you one if you send me a hard drive. You can destroy it with a hammer  
8 and all files really gone. Takes under a minute. Accessed externally to computers." When Petersen  
9 asked whether Spencer felt "bad or anything," Spencer responded, "No, it's been a thing for so long that  
10 it just doesn't affect me[.] I suppose I'm worried legally speaking but otherwise unaffected."

11 16. The following day, Petersen sent Spencer a screen shot from Amazon.com showing the  
12 hard drive he planned to purchase: a Transcend Military Drop Tested 1 TB external hard drive. Spencer  
13 responded: "I hav [sic] that exact one . . . . That's the one I got." Spencer further explained that, if  
14 Petersen sent him the hard drive, Spencer would fill it with child pornography and encrypt it for him.

15 17. Later the same day, Petersen asked whether Spencer had babysat Juvenile Victim 1  
16 ("JV1") lately. Spencer responded that JV1's family had been "weird" lately and that he only liked  
17 babysitting JV1 "because [JV1] lets me molest him." Spencer then described several occasions on  
18 which he had molested JV1, who was then nine years old.

19 18. Messages from October 2016 show Petersen and Spencer setting up a date and time for  
20 Petersen to meet with Spencer in person. Spencer instructed Petersen to come at around 2 pm,  
21 explaining that that would give them sufficient time "to check out the collection." Later that month,  
22 Spencer told Petersen that he would upload some child pornography "from [his] drive" to Dropbox soon.  
23 A few days after that, Spencer wrote to Petersen: "The stuff on my computer is hot as fuck."

24 19. In messages from November 2016, Spencer told Petersen that he was babysitting another  
25 child that weekend. Spencer noted that he could "control and take pictures from [his] iPhone" using his  
26 watch, such that if he "left [the phone] in a room propped up" he could take pictures even if he was not  
27 in the room. Spencer recommended that Petersen try the same thing with children he was babysitting.

1           20.     Other messages show Spencer teaching Petersen how to use the encrypted drive. When  
2 Petersen asked how to use the external hard drive with his computer, Spencer responded, "Just install  
3 Veracrypt on the pc." When Petersen asked how to send files that were on the drive, Spencer  
4 responded: "You download 7z on your computer and throw it into a zipped file with a password. Then  
5 you can upload it direct to the web and send the zip file. If it's encrypted then people can't fuck with it."  
6 Petersen asked whether that method would permit him to send a file directly from the encrypted hard  
7 drive Spencer had made for him, and Spencer responded: "Yep. When you mount it with Veracrypt it  
8 decrypts the files, when you dismount it they re-encrypt."

9           **Other applications found on the iPhone seized from Spencer's room**

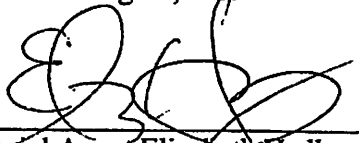
10           21.     My review of the iPhone showed that an application called "Spy Camera" was installed  
11 on it. This application allows the user to take photographs surreptitiously.

12           22.     The iPhone also contained an application with the word "Folder" under the icon. This  
13 application is password-protected.

14           23.     I conducted open-source research on the application labeled as "Folder," and I  
15 determined that it is likely an application known as "Secret Folder & Photo Video Vault Pro." This  
16 application is no longer available on the Apple "App Store" or the Google "Play Store," nor could I find  
17 any other website on which the application was available for download.

18           I declare under penalty of perjury that the foregoing is true and correct to the best of my  
19 knowledge.

20           Executed on this 22nd day of December, 2017, in Washington, DC.

21  
22  
23             
24           Special Agent Elizabeth Hadley  
25           Federal Bureau of Investigation  
26  
27  
28